Sub a1

What is claimed is:

1. A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying the security service; and

processing, in a controller adapted to control communication with the communications channel, the data block according to the security information.

2. The method of claim 1, wherein the processing includes performing cryptographic processing of the data block.

3. The method of claim 1, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

4. The method of claim 1, further comprising:

determining if the security service can be performed by the controller; and

if not, processing the data block according to the security service in a software routine instead of the controller.

5. The method of claim 1, further comprising identifying a security service according to an Internet Protocol security protocol.

6. A method for use in a device including a controller adapted to control communication with a transport medium, comprising:

receiving data from a routine in the device;

sending the data to the controller to perform cryptographic processing of the data; and

after cryptographic processing, transmitting the processed data back to the routine.

7. The method of claim 6, further comprising sending the processed data to the controller at least one more time to perform further cryptographic processing.

8. A method for use in a device including a controller adapted to control communication with a transport medium, comprising:

receiving data from the transport medium;

determining from a portion of the data if cryptographic processing of the data is to be employed; and

performing, in the controller, the cryptographic processing of the data.

9. The method of claim 8, wherein the performing of the cryptographic processing is performed by a cryptographic engine in the controller.

10. The method of claim 8, further comprising:

determining if the cryptographic processing can be performed by the controller; and

performing the cryptographic processing in a software routine instead if the controller is unable to perform the cryptographic processing.

11. An article including a machine-readable storage medium containing instructions for execution in a system including a controller adapted to control communications with a communications channel, the instructions when executed causing the system to:

identify a security service to be performed on data to be transmitted over the communications channel; and

prepare security control information to pass along with the data to the controller to perform processing according to the identified security service.

12. The article of claim 11, the storage medium containing instructions that when executed further causes the system to perform processing according to the identified security service instead of the controller if the security service cannot be performed by the controller.

13. An article including a machine-readable storage medium containing instructions for execution in a system including a controller adapted to control communications with a communications channel, the instructions when executed causing the system to:

receive a data block from the controller;

determine from information in the data block if a security service has been performed on the data block by the controller; and

process the data block if the security service has not been performed on the data block by the controller.

14. The article of claim 13, the storage medium containing instructions that when executed causes the system to retrieve security information associated with the data block and send the data block and security information to the controller to perform the security service.

15. The article of claim 13, the storage medium containing instructions that when executed causes the system to perform the security service on the data block.

16. A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information; and

a cryptographic engine to cryptographically process the data based on the security control information.

17. The controller of claim 16, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

18. The controller of claim 17, further comprising a device adapted to change the contents of the storage device to update the security services information.

19. The controller of claim 18, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

20. The controller of claim 17, wherein the security services information includes security association information.

21. A device coupled to a communications channel, comprising:

an entity capable of generating data for transmission to the communications channel; and

a controller adapted to control communication between the entity and the communications channel, the controller including an engine to modify the data according to a security protocol before transmitting the data to the communications channel.

22. The device of claim 21, wherein the engine is adapted to perform cryptographic processing.

23. The device of claim 21, wherein the controller includes a network controller.

24. The device of claim 21, wherein the entity includes an application process.

25. The device of claim 21, further comprising a routine adapted to generate predetermined security information used by the engine to modify the data according to the security protocol.

26. The device of claim 21, wherein the controller includes a receiving circuit to receive data from the communications channel and security data to identify if the received data is subject to cryptographic processing.

27. The device of claim 26, wherein the controller further includes a cryptographic engine to perform the cryptographic processing on the received data.